Damaris

Damaris SA

PSSI

Damaris SA

PSSI

Version	Auteur : modifications	Date
1.00	AA : Création du document	24/01/2023

Table des matières

1 - INTRODUCTION

Ce document constitue la PSSI (Politique de la sécurité des systèmes d'informations) de Damaris SA.

La société Damaris héberge des solutions de dématérialisation de documents pour le compte de ses clients. Elle propose également la solution Damaris RM en mode On Premise.

A ce titre, elle met en œuvre un certain nombre de « Bonnes pratiques » permettant de garantir la sécurité des données, ainsi que de gérer les incidents éventuels.

2 – LE CONTEXTE

Le périmètre de ce document concerne l'offre « Damaris Cloud ».

Les solutions Damaris RM installées « On Premise » exploitent des ressources non-gérées par la société Damaris et de ce fait, ne peuvent pas être couvertes par cette PSSI.

3 – ELEMENTS STRATEGIQUES

3.1 – LE PERIMETRE DE LA PSSI

Le périmètre de la PSSI chez Damaris concerne en premier point la sécurisation des informations de nos clients traitées sur les serveurs Damaris Cloud.

3.2 – LES ENJEUX ET ORIENTATIONS STRATEGIQUES

Nos clients exploitent les outils Damaris Cloud en ligne pour le traitement et la mise à disposition de leurs documents de gestion.

Les enjeux principaux concernent la continuité de service à nos clients, ainsi que la non-détérioration de leurs données.

De plus, vue la nature parfois très sensible des données, il convient de prévenir des fuites d'informations.

3.3 – LES ASPECTS LEGAUX ET REGLEMNTAIRES

Les données et les documents appartenant à nos clients, le principe réside à offrir l'étanchéité vis-à-vis des autres tiers. Seuls les utilisateurs de nos clients décideront avec qui ils souhaitent partager leurs informations.

Le RGPD est un point central du socle réglementaire de la prestation proposé par Damaris.

3.4 – LES BESOINS DE SECURITE DE NOS CLIENTS

Une fois le serveur mis en production, les besoins concernent essentiellement la continuité de service, la non-destruction des informations, la sécurité d'accès aux informations réservée uniquement aux personnes habilitées et la non-fuite des données.

3.5 – LES ORIGINES DES MENACES

Les menaces peuvent provenir essentiellement des éléments extérieurs, ainsi que de l'intérieur de l'entreprise de nos clients.

Les risques majeures sont la fuite des données ou leur détérioration.

4 – REGLES DE SECURITE

4.1 – ORGANISATION

4.1.1 – Gestion des risques SSI

Une cartographie des risques SSI est établie.

Chaque risque potentielle est catégorisée selon la probabilité de sa survenance et de son impact sur le service.

Elle est revue et mise à jour périodiquement.

4.1.2 – Assurance et certification

La certification principale concerne la norme ISO 27001 liée à l'infrastructure technique utilisée pour les serveurs Damaris Cloud.

La solution Damaris RM est une implémentation de la norme ISO 15489 sur le Records Management. Cette norme est un ensemble de bonnes pratiques archivistiques.

De plus, la société Damaris a souscrit une assurance responsabilité civile « Activités informatiques » auprès d'une compagnie d'assurance basée en France.

4.2 – MISE EN ŒUVRE

4.2.1 – Aspects humains

Les intervenants Damaris sont sensibilisés sur le SSI. Les contrats de travail stipulent la confidentialité de la manipulation des informations de nos clients.

4.2.2 – Gestion des incidents

Le portail Damaris Extranet est mis à la disposition de nos clients et des intervenants Damaris pour signaler les incidents sous la forme de tickets.

Chaque ticket est horodaté, ainsi que toutes les actions qui y sont liées.

Une procédure de gestion des tickets décrit le traitement de chaque incident selon sa gravité, son urgence et permet d'assigner le ticket à la bonne ressource. Le système d'escalade est décrit dans ce mode opératoire.

4.2.3 – Sensibilisation et formation

Les outils d'informations internes de Damaris intègrent de la documentation spécifique concernant la PSSI.

Les intervenants Damaris sont régulièrement invités à prendre connaissance de ces informations mises à jour périodiquement.

4.2.4 – Exploitation

Dans le cadre du RGPD et de la PSSI, nous exploitons les données et les documents uniquement sur les plates-formes prévues à cet effet.

Dès la fin d'un contrat, nous établissons un procès verbale de recette définitive intégrant la destruction des données du client, après l'accord de ce dernier.

4.2.5 – Aspects physiques et environnementaux

Les locaux Damaris sont sécurisés. Aucune personne extérieure ne peut accéder aux locaux sans être accompagnée par une personne de Damaris.

Les serveurs Damaris Cloud se situent dans des Data Centers en France métropolitaine et sont inaccessibles physiquement.

4.3 – TECHNIQUE

4.3.1 – Identification et authentification

La solution Damaris RM propose en standard plusieurs modes d'authentification, selon les souhaits du client et des connecteurs disponibles au sein de son SI.

- Code utilisateur et mot de passe
    - C'est le moyen de connexion classique. A ce niveau, nos clients peuvent déterminer la composition minimale des mots de passe, longueur et contenu, ainsi que la périodicité du renouvellement. Notez qu'il n'est pas possible de réutiliser les anciens mots de passes
- Code utilisateur, mot de passe et jeton (Authentification à deux facteurs)
- Connecteur SAML SSO V2

- Connecteur Azure AD
- Connecteur Kerberos SPNego
- Connecteur OpenID

Pour les connecteurs SSO, nous mettons à disposition des méthodes de synchronisation des comptes utilisateurs avec l'annuaire du client.

4.3.2 – Contrôle d'accès logique

Le contrôle d'accès est géré avec les mécanismes suivants :

- L'accès à une typologie de documents selon le service de rattachement de l'utilisateur
    - Par exemple, la personne fait partie du service administratif et financier et du coup elle a accès aux facture fournisseurs
- La restriction d'accès selon les critères (Les métadonnées). Dans ce cas, il est possible de n'octroyer d'accès que selon des valeurs d'index. Par exemple, un groupe d'utilisateurs ne voit que les comptes fournisseurs dont il en a la gestion
- Les documents personnels. Seul la personne qui archive le document peut y accéder (Diffusion restreinte)

4.3.3 – Journalisation

La solution Damaris RM est basée sur la norme ISO 15489. Cette norme intègre la traçabilité de toutes les actions effectuées dans le système.

Le journal détaillé est disponible pour les administrateurs du système.

5 – PLAN D'ACTION

5.1 – SURVEILLANCE ET ALERTING

Une surveillance s'effectue toutes les 5 minutes pour vérifier si le service est toujours en ligne. En cas de défaillance, une alerte est envoyée à l'équipe Damaris pour démarrer les actions nécessaires à la remise en route du serveur. Les horaires de disponibilité et des dépannages dépendent du contrat de service.

5.2 – SAUVEGARDES

Les serveurs Damaris sont sauvegardées quotidiennement. Les fichiers de sauvegarde sont cryptés sur un serveur se trouvant dans un autre Data Center éloigné de plus de 50 km du serveur de production.

Nous conservons une sauvegarde pour les 7 derniers jours, les 4 dernières semaines et les 12 derniers mois.

5.3 – GESTION DES EQUIPEMENTS

Nous exploitons une infrastructure propre à Damaris, sans recourir à de la mutualisation des équipements avec d'autres prestataires.

Périodiquement, nous procédons à une revue de l'infrastructure pour prendre les mesures nécessaires quant au maintien, à la mise à jour ou à l'arrêt d'un équipement.

5.4 – ISOLEMENT DES FLUX

La solution Damaris RM garantit l'étanchéité des informations entre les différents clients.

Il existe plusieurs niveaux d'isolement, dépendant du contrat de service :

- Un serveur mutualisé entre plusieurs clients : Damaris RM utilise le mécanisme de multi-sociétés. Un utilisateur nommé ne pouvant faire partie que d'une seule société et n'accède qu'aux documents de sa société
- Un serveur mutualisé, avec une instance Damaris RM dédiée : Dans ce cas, la base de données et le coffre-fort sont dédiés au client. Nous ne mutualisons que l'infrastructure technique
- Un serveur dédié à un client : L'infrastructure technique ne contient que les données d'un seul client

5.5 – POLITIQUE ANTIVIRALE

Un antivirus est installé sur chaque équipement, poste de travail et serveur.

5.6 – ROADMAP

Le roadmap Damaris est organisé pour une livraison bimestrielle de versions de la solution. Voici les dates prévisionnelles établies pour chaque année :

- Septembre de chaque année : v X.0 : Version majeure
- Novembre : v X.1 : première version mineure
- Janvier : v X.2 : Deuxième version mineure
- Mars : v X.3 : Troisième version mineure
- Mai : v X.4 : Quatrième version mineure
- Juillet : v X.5 : Cinquième version mineure